J Inf Process Syst, Vol.16, No.4, pp.760~773, August 2020
https://doi.org/10.3745/JIPS.04.0178

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric

Junho Jeong[*], Donghyo Kim[**], Byungdo Lee[***], and Yunsik Son[**]

Abstract

When a crime occurs, the information necessary for solving the case, and various pieces of the evidence needed to prove the crime are collected from the crime scene. The tangible residues collected through scientific methods at the crime scene become evidence at trial and a clue to prove the facts directly against the offense of the suspect. Therefore, the scientific investigation and forensic handling for securing objective forensic in crime investigation is increasingly important. Today, digital systems, such as smartphones, CCTVs, black boxes, etc. are increasingly used as criminal information investigation clues, and digital forensic is becoming a decisive factor in investigation and trial. However, the systems have the risk that digital forensic may be damaged or manipulated by malicious insiders in the existing centralized management systems based on client/server structure. In this paper, we design and implement a blockchain based digital forensic management model using Hyperledger Fabric and Docker to guarantee the reliability and integrity of digital forensic. The proposed digital evidence management model allows only authorized participants in a distributed environment without a central management agency access the network to share and manage potential crime data. Therefore, it could be relatively safe from malicious internal attackers compared to the existing client/server model.

Keywords

Blockchain, Digital Evidence Management, Digital Forensic, Hyperledger Fabric, Smart Contract

1. Introduction

A Policing is one of the important factors for building a secure smart community system. Recently, the policing has been developing into smart community policing using information and communication technologies (ICT). Especially, crime investigation collects various information needed to solve cases, and various types of evidence to prove a crime when the crime occurs. Thus, after collecting tangible residues, the victim's status, and behavioral evidence at the scene of the incident, the basis of scientific investigation is to analyze them scientifically and use the results.

Therefore, records and archives of forensic have been very important in criminal investigation. The importance of keeping forensic evidence is well documented as evidenced by well-known unsolved case in the United Kingdom [1]. In 1981, in England, a 14-year-old girl was found raped and murdered, but the case had been remained unsolved. After 20 years the police were able to arrest the suspect by the

Manuscript received October 11, 2019; first revision April 9, 2020; second revision May 30, 2020; accepted June 14, 2020.

Corresponding Author: Yunsik Son (sonbug@dongguk.edu)

[*] Dept. of Computer Science and Engineering, Kongju National University, Cheonan, Korea (yanyenli@kongju.ac.kr)

[**] Dept. of Computer Science and Engineering, Dongguk University, Seoul, Korea (donghyo@dongguk.edu, sonbug@dongguk.edu)

[***] Dept. of Police Science, Seoul Digital University, Seoul, Korea (leebd84@sdu.ac.kr)

Junho Jeong and Donghyo Kim have contributed equally to this study.

samples taken from the girl’s body at that time.

The importance of chain of custody (CoC) is well documented in the O. J. Simpson case in the United States. The forensic presented to the court in this case showed that the transfer process had not been tampered with and proved that the process was perfect [2]. In Korea, the criminal forensics of the serial murders, which remained unresolved for 33 years, has been preserved to this day. This has recently been used to limit the potential culprits of the case [3]. In other words, recording and keeping evidence is a very important factor in criminal investigations. Investigating a crime means resolving the incident by collecting and analyzing on-site various types of evidence based on the condition and behavior of the offender and the victim demonstrating the crime.

Today, smartphones, CCTVs, black boxes, etc., are increasingly used as criminal information investigation clues, and digital evidence is becoming a decisive factor in investigation and trial [4]. Table 1 shows the numbers of sources of digital evidence by 2018. Since 2009, with the development of electronic device technology, the spread of smartphones has increased, and the proportion of clues or evidence in criminal investigations is increasing. In other words, the number of cases where CCTV, black box, etc., are proved to be important evidence in criminal investigations is increasing, and the use of digital evidence and the number of referrals in criminal investigations is increasing [5].

Table 1. Number of sources of digital evidence in Korea

Year	Sum	PC, laptop	CCTV, navigation	Smartphone	Database
2013	11,200	3,138	483	7,332	247
2014	14,899	3,079	510	10,656	654
2015	24,295	3,357	712	19,526	700
2016	32,281	3,923	794	26,408	1,156
2017	36,060	4,198	867	30,238	757

On the other hand, an increase in the number of sources of digital evidence in criminal investigations means that there is a lot of information to be kept and managed. Therefore, standard criminal investigation method and evidence management system need to be established. Accordingly, various policies and technologies are researched in many countries to establish safe and reliable crime investigation methods and digital evidence management system.

However, in Korea, due to the independent operation guidelines of each local police agency, there is no standard best practice in the operation of digital evidence management system. In particular, the investigating agency in the field can investigate the case and obtain digital evidence through arbitrary submission or seizure search. This digital evidence can be collected by duplicating the original and verifying its integrity through hash values. However, many physical storage devices are acquired.

In this case, the software data is stored and managed in the physical storage obtained through the search until it is submitted to court and delivers the physical storage if necessary. Therefore, it has a problem in that the data stored in the physical storage device is exposed to damage and manipulation [6]. In this process, there is a problem that the CoC is broken and the digital evidence collected and analyzed cannot be adopted hardly as legal evidence due to the lack of reliability of the digital evidence.

Therefore, there was a study to analyze the problems in practice by analyzing the digital evidence system to examine the reliability verification problems of digital evidence [7]. In addition, this study analyzed the overall process that can meet the speed and confidentiality of digital forensic investigation based on the characteristics of the digital forensic system required in practice.

In another study, there was a management plan that considered the life cycle of digital evidence [8]. It was a study to effectively solve the problem of deletion or disposal of evidence due to lack of space. This study analyzed the necessity and utility of integrated management for the large-capacity and diversified evidence. However, this system could be effective against malicious external attacks, but it is inefficient for internal attack.

The client/server environment system refers to a network structure in which a client works with a separated server that is a provider of service resources. In general, since data is stored through a database existing in the central server, it operates in a closed structure between users. Therefore, there is a disadvantage that the central server does not prove the integrity and transparency of the data when the attack or the data is modified by a malicious attacker. In addition, for transaction management, it is necessary to perform a transaction verification using a third-party certification authority. In addition, as the number of devices connected to the server increases, the request and data transmission of the devices may place a heavy load on the server providing a specific service and function.

In this paper, we propose a management model of blockchain-based digital evidence and implemented it using Hyperledger Fabric [9]. This paper is organized as follows. Section 2 introduces the related works about the digital forensic and blockchain. And we propose a digital evidence management model in Section 3. Section 4 analyzes the results of the implementation of the proposed model. Finally, we Section 5 concludes the paper.

2. Related Works

2.1 Digital Crime Investigation Process in Korea

Today, the digital criminal investigation process in Korea has generally the seven stages. The stages include initial survey, investigation, arrest, the closing of investigation, request for analysis, transfer of digital evidence and investigation, and trial. Fig. 1 shows the criminal investigation process in Korea.

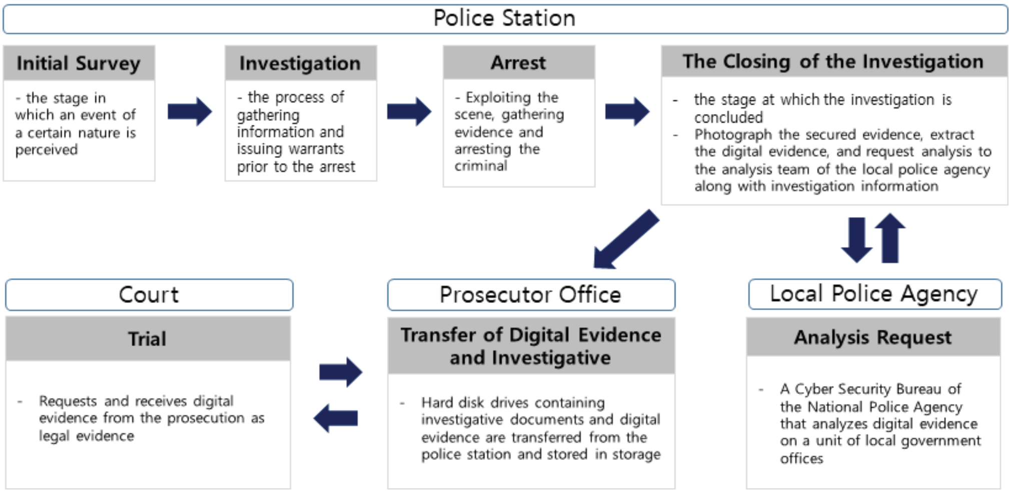

Police Station
Initial Survey
- the stage in which an event of a certain nature is perceived
Investigation
- the process of gathering information and issuing warrants prior to the arrest
Arrest
- Exploiting the scene, gathering evidence and arresting the criminal
The Closing of the Investigation
- the stage at which the investigation is concluded
- Photograph the secured evidence, extract the digital evidence, and request analysis to the analysis team of the local police agency along with investigation information
Court
Trial
- Requests and receives digital evidence from the prosecution as legal evidence
Prosecutor Office
Transfer of Digital Evidence and Investigative
- Hard disk drives containing investigative documents and digital evidence are transferred from the police station and stored in storage
Local Police Agency
Analysis Request
- A Cyber Security Bureau of the National Police Agency that analyzes digital evidence on a unit of local government offices

Fig. 1. Digital criminal investigation process in Korea.

The initial survey is the first action when an incident occurs, and the field investigation agency recognizes what kind of event it is and starts an investigation. The investigation stage then issues a warrant, collecting information on the case, convicting the suspect, and the culprit before the arrest. At the scene of the crime, criminal evidence is collected, and the culprits are arrested based on the warrant. If the suspect is arrested and the investigation is terminated, the investigators will collect additional criminal evidence at the scene. The evidence, along with the investigation information, is analyzed by the local police department's analysis team and the results are obtained. After that, the investigative documents, the results of the criminal evidence analysis, and the physical storage device storing the digital evidence are transferred to the prosecutor's office and stored. Finally, the proceedings are submitted as court evidence at the time of trial.

In the transfer of investigation documents and evidence, prosecutors examine only the documents in the case to determine the investigation, based on the trust of the entire criminal justice system. Thus, the procedure has a risk that a malicious insider could compromise or manipulate the digital evidence of the physical storage device. In this case, there is a problem in that it cannot be used as legal evidence because it cannot maintain continuity of management from the point of view of CoC [2,6].

2.2 Digital Evidence Management Research

Various studies have been continuously attempted to increase the originality, integrity, and authenticity of criminal digital evidence obtained through random submission or seizure search. Recently, research have been conducted to understand the characteristics of digital data, to establish an efficient management environment based on digital forensic, and to perform integrated management [8]. As shown in Fig. 2, this study classifies and links the system into three crime investigation management areas: National Police Agency's case management system, National Police Agency's digital evidence management system, and Public Prosecutor's Office digital evidence management system. And it uses national transmission network to manage digital evidence and investigation information.

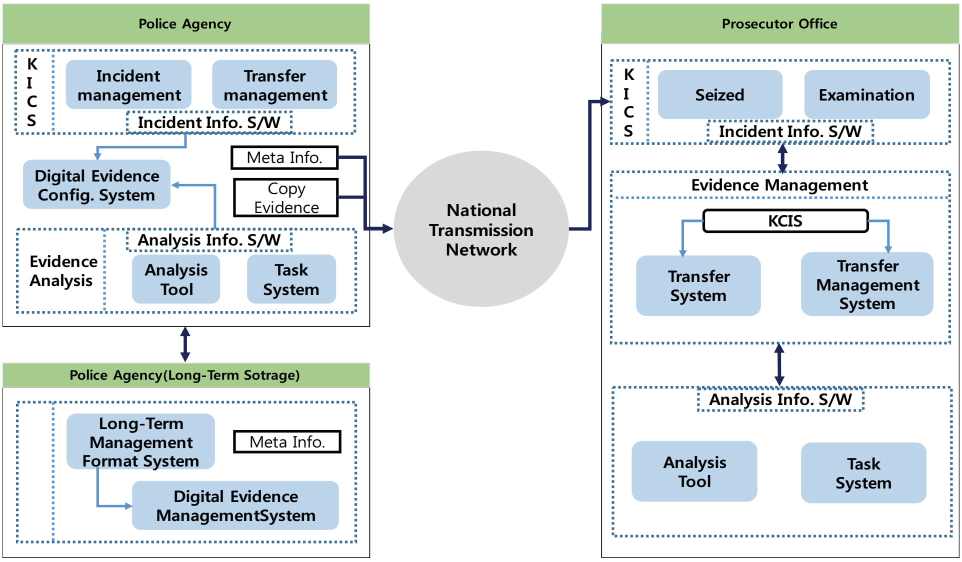


Fig. 2. Digital evidence integrated management system. Adapted from [8].

However, this digital evidence integrated management system is a centralized system in a client/server environment. Therefore, authentication must be performed using a third party to manage transactions. In addition, a server for storing and managing digital evidence and investigation information is integrated. Therefore, if the central server is attacked, the operation and the important investigation information of the organization can be leaked, and thus the continuity of management cannot be maintained. In order to solve this problem, the transfer of digital evidence and investigation documents will be stored and shared in all networks, and the application of high transparency and reliability technology should be required.

2.3 Blockchain & Hyperledger Fabric

Blockchain, represented by Bitcoin is implemented in such a way that the participant collectively records and manages data by distributing the ledger to a peer-to-peer network rather than to a central server of a specific organization [10]. In this case, the data is stored in a distributed manner to several sites, several countries, or several institutions. In case of a write request from the user, the data is shared to all the systems.

In other words, the blockchain is a data structure for implementing distributed ledgers. It connects all the transaction blocks that have been agreed and validated by network participants to the most recently created block from the beginning of the chain. It is a technology that can manage the same transaction by distributing it to all network members. The verification of the transaction is performed by using a third-party certification authority to manage the transaction in the client/server environment, while in the blockchain network, the verification of the contents in the ledger is performed by digital signature and smart contract.

Blockchains are categorized into three areas: public blockchain, private blockchain, and consortium blockchain [11]. The digital evidence management model in the proposed study applies the Hyperledger Fabric to achieve the goal of this study. The Hyperledger Fabric is a consortium blockchain framework in which several organizations form a consortium and only authorized organizations can join the network. The framework is one of the Linux Foundation's projects, Hyperledger, an open-source framework for building blockchain network infrastructure for business-to-business (B2B) and business-to-consumer (B2C) transactions [9]. Unlike Bitcoin and Ethereum, the leading public chain frameworks, Hyperledger Fabric is not a cryptocurrency based, but a consortium blockchain technology for business.

In addition, in contrast to public blockchains where anyone can participate, Hyperledger Fabric utilizes digital certificate and public key cryptography technology based on public key infrastructure (PKI) technology to manage affiliation, identity, and access permission and role of participating users in the network. Therefore, through the technique, the integrity of network participants can be proved, and only users who have access to the network by channel can participate in the blockchain network to provide privacy and confidentiality between the participants [12,13]. Fig. 3 shows the architecture of the model.

This means that not only all information can be shared equally, but also that the digital evidence and investigative information, which are important information, can be composed only among participants who want to share channels and create and share a separate ledger. Hyperledger Fabric generally consists of a blockchain network and a certificate authority server/client. Membership information, such as peer's authority and orderer's authority, defined in the client are registered in the certification authority server [14,15]. In addition, cryptographic data such as digital certificates, public keys, and private keys, genesis blocks, and transaction generators can be created and distributed to the Hyperledger Fabric network and maintained based on this.

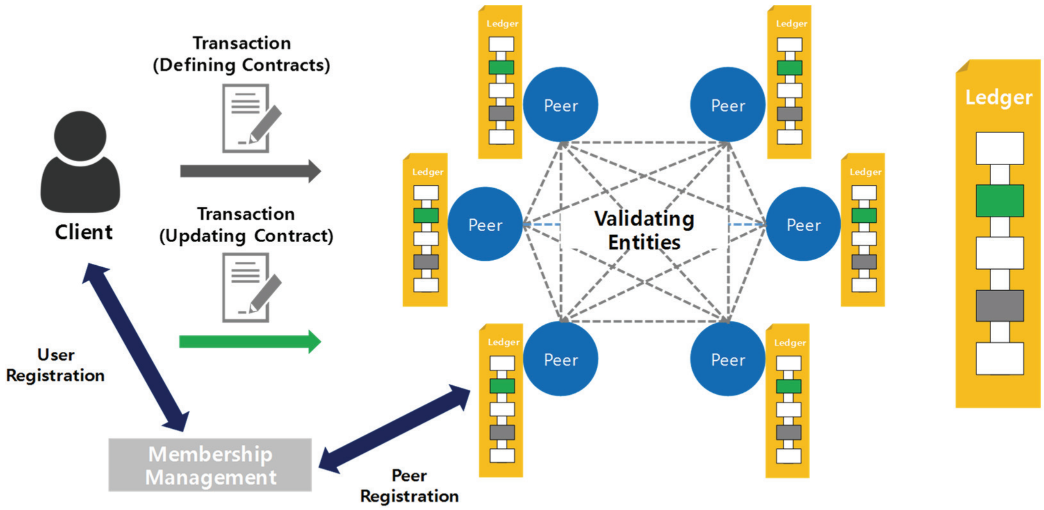


Fig. 3. Hyperledger Fabric platform model architecture.

Peer refers to a node in a Hyperledger Fabric network. Depending on the role played, “endorsing peer” performs the verification of the transaction that performs the smart contract, “committing peer” performs the verification of the latest block, and “anchor peer” connected to communicate with other institutions and receives the latest block connected to the orderer. It consists of “leader peer” that transmits to other peers in the organization. The orderer is a node that collects, sorts, and generates the actual block after the endorsing peer has verified the transaction that executes the smart contract. This process is called consensus [12,16].

As this work is separated and processed, it is possible to reduce the load of peers executing and verifying transactions, and parallel processing to perform various tasks is possible. Therefore, this paper also utilizes the technology of Hyperledger Fabric for effective and reliable digital evidence management.

2.4 Smart Contract in Hyperledger Fabric

Smart contract is an essential part of the digital evidence management model presented in this paper. It is a technology that can be easily and conveniently concluded and modified without an intermediary and uses the characteristics of distributed ledger technology (DLT). Thus, various types and forms of contract processing are possible, such as financial transactions, certification and contract notarization [12,17]. In Hyperledger Fabric, the source code that implements smart contracts is called chaincode. Installed on peers in a preconfigured network and used to execute transactions as a transaction.

If necessary, a plurality of chain cords may be installed in a peer, and a plurality of chain cords may be installed in a single peer. Unlike general smart contract technologies, Hyperledger Fabric’s smart contracts are classified into two types: system chaincode executed at the system level and developer chaincode that access the ledger at the application level.

A total of five system chaincodes are provided to facilitate development by directly instructing Hyperledger Fabric network systems [18]. Each chain code is as follows.

(1) Query system chaincode (QSCC) reads the hash value, block number, and transaction ID of the stored block of the blockchain.

(2) The endorsement system chaincode (ESCC) compares a user's transaction execution result and, if it is correct, guarantees the transaction's result with its own certificate.
(3) The validation system chaincode (VSCC) validates the existence of digital certificates in accordance with the data read and transaction policy of the transaction.
(4) Configuration system chaincode (CSCC) creates channel and joins peer and orderer to channel.
(5) Lifecycle system chaincode (LSCC) performs chaincode installation and peer data initialization on the peer.

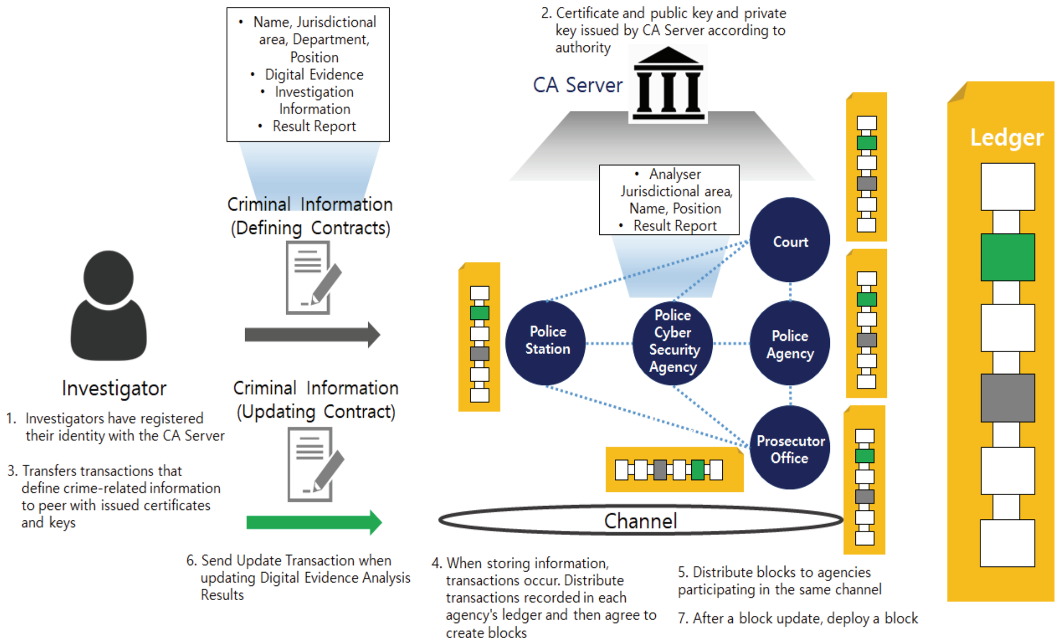
Developer chaincode, on the other hand, is a source code that directly executes contracts and can be written through general programming languages Go, JavaScript, and Java [19].

3. Proposed Digital Evidence Management Model

3.1 Design of the Process for Digital Forensic using Hyperledger Fabric

The digital evidence management model proposed in this paper aims to overcome the problems of research limited to the existing server/client environment by blockchain network framework Hyperledger Fabric and to manage transparent and reliable digitalized evidence.

The Hyperledger Fabric provides a channel system between participating organizations and organizations in the blockchain, and can efficiently manage participation rights, identities, and roles in the blockchain based on PKI technology. Based on this, there is an advantage of providing privacy and confidentiality of institutions, organizations, and users. Therefore, it could be providing the privacy and confidentiality of limited institutions like the proposed model and supports the optimal function to improve the reliability of the shared data.


• Name, Jurisdictional area, Department, Position
• Digital Evidence
• Investigation Information
• Result Report
Criminal Information (Defining Contracts)
Investigator
Criminal Information (Updating Contract)
CA Server
• Analyser Jurisdictional area, Name, Position
• Result Report
Court
Police Station
Police Cyber Security Agency
Police Agency
Prosecutor Office
Channel
Ledger

1. Investigators have registered their identity with the CA Server

2. Certificate and public key and private key issued by CA Server according to authority

3. Transfers transactions that define crime-related information to peer with issued certificates and keys

4. When storing information, transactions occur. Distribute transactions recorded in each agency's ledger and then agree to create blocks

5. Distribute blocks to agencies participating in the same channel

6. Send Update Transaction when updating Digital Evidence Analysis Results

7. After a block update, deploy a block

Fig. 4. The proposed digital evidence management system model process architecture.

Fig. 4 shows the process of the proposed digital evidence management model. Provincial Police Agencies, National Police Agency, Cyber Analyst Teams, Prosecutors' Office and Courts form consortiums to participate in blockchain channels and share digital evidence. The process begins with the field investigator registering the digital evidence collected in the blockchain network. Digital evidence information includes case numbers, case information, jurisdictions, registrants, investigation records, analysis results, and dates. However, the step 1–2 that is for identity registration and certificate issuance process is performed only by newly participating organizations.

After that, the identification confirmation of the registered digital evidence information registrant and the digital evidence information are verified, and the verified evidence information is generated through a chain code, which is a smart contract predefined in the peer, and distributed to all agencies. Accordingly, all agencies can share the registered digital evidence information through distributed blocks. In addition, once blocks are created. The blocks cannot be deleted and modified to increase the transparency and reliability of digital evidence.

3.2 Design of Hyperledger Fabric Network for the Proposed System

The Hyperledger Fabric network consists of digital evidence registrants (clients), peers, orders, channels, chaincodes, and membership service providers. Fig. 5 illustrates the network for the proposed system. Peers are chained together by a consortium of Provincial Police Agencies, National Police Agency, Cyber Analyst Teams, Prosecutors' Office and Courts that handle criminal investigation information. To do this, we use Docker and Hyperledger Fabric, container-based open source virtualization platforms. It maintains peers, orders, and channels using membership information, institutions, digital certificates, public keys, and private key cryptography techniques [20].

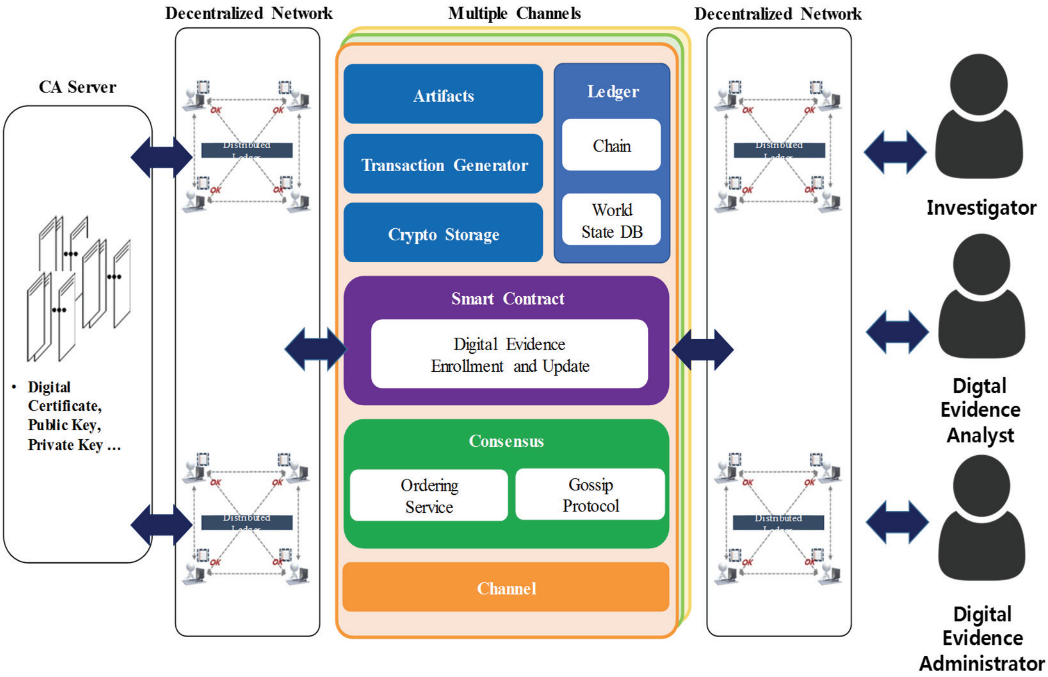


Fig. 5. The proposed digital evidence management system model architecture.

Therefore, the membership service provider may verify the identity of the registrant as a participant in the organization when a digital forensic registrant registers an identity on a Hyperledger Fabric network. It also issues encrypted data and accesses to the network.

Subsequently, when the registered registrant submits the digital forensic registration transaction, the chaincode installed in the peer is executed to record the transaction in the ledger, and the transactions are distributed to all endorsement peers through the anchor peers connected to each peer. As a result, all endorsement peers verify the distributed transaction, generate a block, and perform distribution again.

4. Implementation and Analysis

The proposed system model implemented based on Hyperledger Fabric a blockchain network infrastructure framework and Docker that is an s/w virtualization platform in this paper. Table 2 show the detail environment for the implementation. The first step in the implementation of criminal digital evidence management blockchain network is to establish the organization and authority of peers and orderers using membership service providers. In order to set the authority of peer using membership service provider, the authentication server was maintained as a Docker container. The *yaml* file for setting permissions is mounted as a container on the Host. Therefore, it was issued when a request for authorization and PKI-based encryption data was received from the outside. Therefore, in the proposed blockchain network, for each individual peer organization, the National Police Agency, the Cyber Analysis Center, Prosecutor’s Office, Court, and National Police Agency set to the same level of authority, and digital certificates, public keys, private keys, genesis block, transaction generator encrypted data was generated. In addition, a Docker container is constructed based on the generated encrypted data and network peers and orderer are always enabled. Containers of peers of the local police agency and the Cyber Analysis Center, the Prosecutor’s Office, the Courts, and the police agency joined to the channel so that they are configured in the same network.

Table 2. The detail environment for the implementation

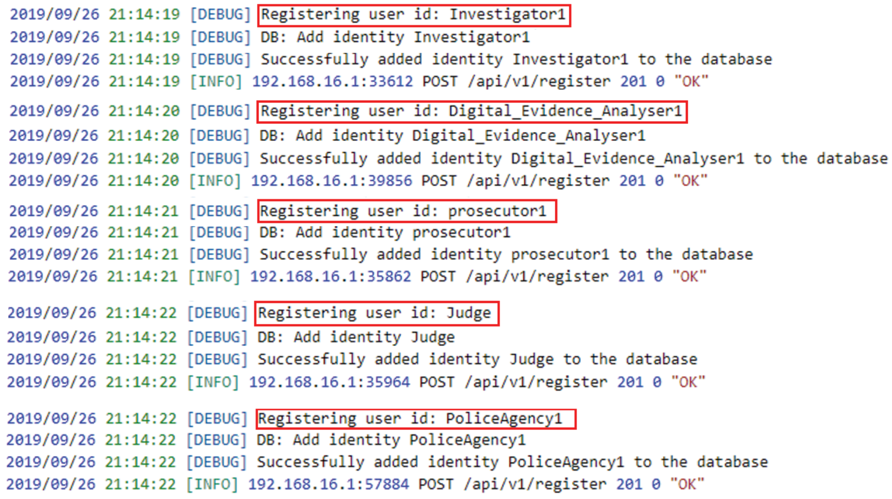
Software	Version
Ubuntu	V16.04LTS
Hyperledger Fabric	V1.2
Golang	V11.4
Docker	V18.06.1-ce
Docker-Compose	V8.11

Fig. 6 shows the result of obtaining user authority by requesting identity registration from the authentication server of each institution to register the user identity to each peer such as the police department, the Prosecutor's Office, the digital cyber analysis team, and the Court of the blockchain network. The red box in Fig. 6 shows that all the peers in the digital evidence management system have been successfully registered.

Fig. 7 also shows the digital certificate provided by the authentication server based on the registered identity. When registering the identity, the authentication server issues a separate digital certificate, public key, and private key for each institution, and uses it to verify the identity in the blockchain network.

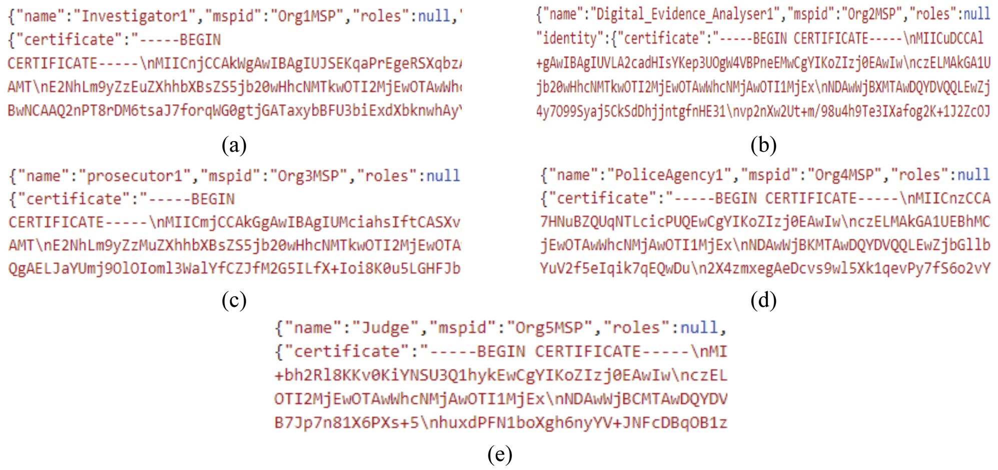
And the chaincodes are setup to perform smart contracts to record digital evidence and investigation-related information by investigators on the blockchain network at all peers.

The chaincode set in the peer executes the smart contract by passing the argument to the corresponding function created in the blockchain network when the registration transaction is submitted. The contents of this transaction include case information, jurisdiction, registrant, investigation record, and date. The chaincode consists of an Init function to initializes and records digital evidence and investigation-related information, an Invoke function to update evidence information recorded, a Query function to retrieve recorded information, and finally DELETE function to remove the data by identifier in the ledger.



```
2019/09/26 21:14:19 [DEBUG] Registering user id: Investigator1
2019/09/26 21:14:19 [DEBUG] DB: Add identity Investigator1
2019/09/26 21:14:19 [DEBUG] Successfully added identity Investigator1 to the database
2019/09/26 21:14:19 [INFO] 192.168.16.1:33612 POST /api/v1/register 201 0 "OK"

2019/09/26 21:14:20 [DEBUG] Registering user id: Digital_Evidence_Analyser1
2019/09/26 21:14:20 [DEBUG] DB: Add identity Digital_Evidence_Analyser1
2019/09/26 21:14:20 [DEBUG] Successfully added identity Digital_Evidence_Analyser1 to the database
2019/09/26 21:14:20 [INFO] 192.168.16.1:39856 POST /api/v1/register 201 0 "OK"

2019/09/26 21:14:21 [DEBUG] Registering user id: prosecutor1
2019/09/26 21:14:21 [DEBUG] DB: Add identity prosecutor1
2019/09/26 21:14:21 [DEBUG] Successfully added identity prosecutor1 to the database
2019/09/26 21:14:21 [INFO] 192.168.16.1:35862 POST /api/v1/register 201 0 "OK"

2019/09/26 21:14:22 [DEBUG] Registering user id: Judge
2019/09/26 21:14:22 [DEBUG] DB: Add identity Judge
2019/09/26 21:14:22 [DEBUG] Successfully added identity Judge to the database
2019/09/26 21:14:22 [INFO] 192.168.16.1:35964 POST /api/v1/register 201 0 "OK"

2019/09/26 21:14:22 [DEBUG] Registering user id: PoliceAgency1
2019/09/26 21:14:22 [DEBUG] DB: Add identity PoliceAgency1
2019/09/26 21:14:22 [DEBUG] Successfully added identity PoliceAgency1 to the database
2019/09/26 21:14:22 [INFO] 192.168.16.1:57884 POST /api/v1/register 201 0 "OK"
```

Fig. 6. Identification using membership service.



```
{"name":"Investigator1","mspid":"Org1MSP","roles":null,
{"certificate":"-----BEGIN
CERTIFICATE-----\nMIICnjCCAkWgAwIBAgIUJSEKqaPrEgeRSXqbz
AMT\nE2NhLm9yZzEuZXhhbXBsZS5jb20wHhcNMTkwOTI2MjEwOTAwWh
BwNCAAQ2nPT8rDM6tsaJ7forqWG0gtjGATaxybBFU3biExdXbknwhAy
```

(a)

```
{"name":"Digital_Evidence_Analyser1","mspid":"Org2MSP","roles":null
"identity":{"certificate":"-----BEGIN CERTIFICATE-----\nMIICuDCCAl
+gAwIBAgIUVLA2cadHIsYKep3UOgW4VBPneEMwCgYIKoZIzj0EAwIw\nczELMAkGA1U
jb20wHhcNMTkwOTI2MjEwOTAwWhcNMjAwOTI1MjEx\nNDAwWjBXMTAwDQYDVQQLEwZj
4y7O99Syaj5CkSdDhjjntgfnHE31\nvp2nXw2Ut+m/98u4h9Te3IXafog2K+1J2ZcOJ
```

(b)

```
{"name":"prosecutor1","mspid":"Org3MSP","roles":null
{"certificate":"-----BEGIN
CERTIFICATE-----\nMIICmjCCAkGgAwIBAgIUMciahsIftCASXv
AMT\nE2NhLm9yZzMuZXhhbXBsZS5jb20wHhcNMTkwOTI2MjEwOTA
QgAELJaYUmj9OlOIoml3WalYfCZJfM2G5ILfX+Ioi8K0u5LGHFJb
```

(c)

```
{"name":"PoliceAgency1","mspid":"Org4MSP","roles":null
{"certificate":"-----BEGIN CERTIFICATE-----\nMIICnzCCA
7HNuBZQUqNTLcicPUQEwCgYIKoZIzj0EAwIw\nczELMAkGA1UEBhMC
jEwOTAwWhcNMjAwOTI1MjEx\nNDAwWjBKMTAwDQYDVQQLEwZjbGllb
YuV2f5eIqik7qEQwDu\n2X4zmxegAeDcvs9wl5Xk1qevPy7fS6o2vY
```

(d)

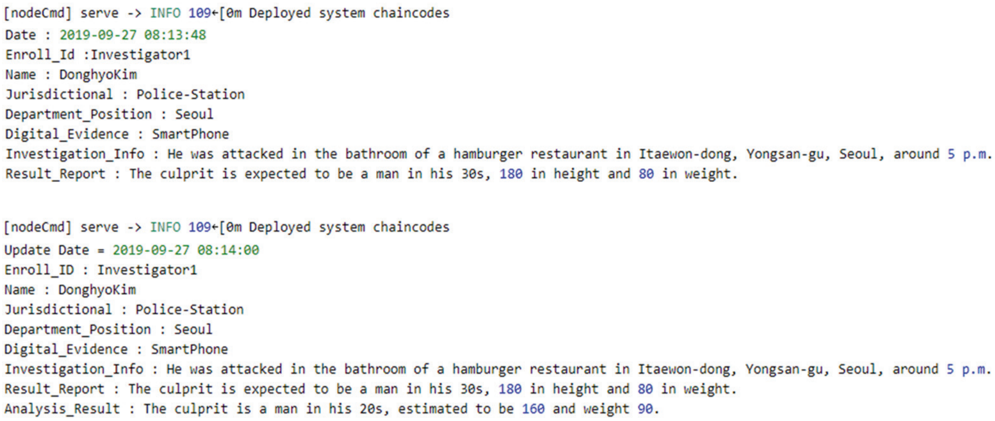
```
{"name":"Judge","mspid":"Org5MSP","roles":null,
{"certificate":"-----BEGIN CERTIFICATE-----\nMI
+bh2Rl8KKv0KiYNSU3Q1hykEwCgYIKoZIzj0EAwIw\nczEL
OTI2MjEwOTAwWhcNMjAwOTI1MjEx\nNDAwWjBCMTAwDQYDV
B7Jp7n81X6PXs+5\nhuxdPFN1boXgh6nyYV+JNFcDBqOB1z
```

(e)

Fig. 7. Digital certificate issued after identity registration: (a) police station, (b) cyber police security, (c) the Prosecutor's Office, (d) police agency, and (e) the Court.

Identifying the digital evidence registrant through the chaincode is identified by Enroll_Id, the registrant's network ID. When the digital evidence registrant passes the registration transaction to the blockchain network, the digital evidence is registered in the ledger through chaincode execution. In addition, the chaincode is executed by the police agency peers to record all transactions identically in the ledger owned by peers participating in the channel.

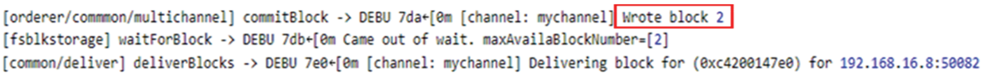
Fig. 8 shows the result of recording and updating digital evidence using the identifier ID in the established chaincode. Transactions are shared among all peers using anchor peers that communicate with other peers. When chaincode is executed on all peers and the transaction is shared, all nodes agree to create a block. And all peers participating in the channel will share the same criminal digital evidence registration information.



```
[nodeCmd] serve -> INFO 109←[0m Deployed system chaincodes
Date : 2019-09-27 08:13:48
Enroll_Id :Investigator1
Name : DonghyoKim
Jurisdictional : Police-Station
Department_Position : Seoul
Digital_Evidence : SmartPhone
Investigation_Info : He was attacked in the bathroom of a hamburger restaurant in Itaewon-dong, Yongsan-gu, Seoul, around 5 p.m.
Result_Report : The culprit is expected to be a man in his 30s, 180 in height and 80 in weight.

[nodeCmd] serve -> INFO 109←[0m Deployed system chaincodes
Update Date = 2019-09-27 08:14:00
Enroll_ID : Investigator1
Name : DonghyoKim
Jurisdictional : Police-Station
Department_Position : Seoul
Digital_Evidence : SmartPhone
Investigation_Info : He was attacked in the bathroom of a hamburger restaurant in Itaewon-dong, Yongsan-gu, Seoul, around 5 p.m.
Result_Report : The culprit is expected to be a man in his 30s, 180 in height and 80 in weight.
Analysis_Result : The culprit is a man in his 20s, estimated to be 160 and weight 90.
```

Fig. 8. Transaction that adds digital.

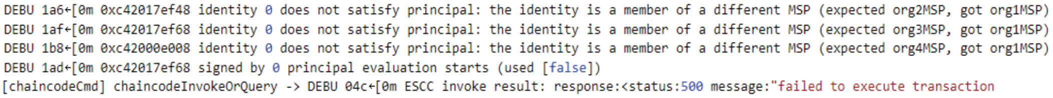
Fig. 9 shows the result of registration and update of all peers participating in the channel. It could be seen that a total of two blocks have been updated and waiting for block generation. As such, it is impossible to modify the digital evidence in which the block was generated, and if there is a modification, the updated contents are recorded in the block, making it difficult to manipulate data by insiders. Even if the digital evidence is corrected by an insider, all the records remain, which increases the reliability of the evidence.



```
[orderer/commmon/multichannel] commitBlock -> DEBU 7da←[0m [channel: mychannel] Wrote block 2
[fsblkstorage] waitForBlock -> DEBU 7db←[0m Came out of wait. maxAvailaBlockNumber=[2]
[common/deliver] deliverBlocks -> DEBU 7e0←[0m [channel: mychannel] Delivering block for (0xc4200147e0) for 192.168.16.8:50082
```

Fig. 9. Block generated by updating transactions.

In addition, in the case of an external attacker accessing the blockchain network and attacking digital evidence recorded in the ledger, as shown in Fig. 10, the user whose identity is not verified cannot modify the transaction and chaincode. In other words, the proposed model can provide high reliability of the crime digital evidence because it is not possible to modify the records stored in the ledger in the peer to which it belongs, as well as the external attackers and the constituent nodes of the crime digital evidence management model.



```
 DEBU 1a6←[0m 0xc42017ef48 identity 0 does not satisfy principal: the identity is a member of a different MSP (expected org2MSP, got org1MSP)
 DEBU 1af←[0m 0xc42017ef68 identity 0 does not satisfy principal: the identity is a member of a different MSP (expected org3MSP, got org1MSP)
 DEBU 1b8←[0m 0xc42000e008 identity 0 does not satisfy principal: the identity is a member of a different MSP (expected org4MSP, got org1MSP)
 DEBU 1ad←[0m 0xc42017ef68 signed by 0 principal evaluation starts (used [false])
[chaincodeCmd] chaincodeInvokeOrQuery -> DEBU 04c←[0m ESCC invoke result: response:<status:500 message:"failed to execute transaction
```

Fig. 10. Ledger update and block generation using unregistered identity.

5. Conclusion and Future Works

Nowadays, we have a risk that a malicious insider could compromise or manipulate the digital evidence of the physical storage device. In this case, it causes a problem in that it cannot be used as legal evidence because it cannot maintain continuity of management from the point of view of CoC. Therefore, the digital evidences that are difficult to analyze are not used as legal evidence because the continuity of management is not guaranteed.

Recently it has been various studies to enable a transparent and reliable management of criminal digital evidence. However, in Korea, the crime digital evidence management system is centrally operated in an integrated server/client environment and is being researched to advance it. The centralized system is not effective for the CoC because the investigation information of the relevant institution can be leaked or manipulated when the central server is attacked, and it is also vulnerable to attacks by insiders. Therefore, a new crime digital evidence management model that is different from the existing system is required.

In this study, we proposed a digital forensic management model that can share and manage data by accessing a network in a distributed environment where only authorized participants participate. The data of digital forensic written once by creating a block cannot be modified and deleted by any user, and has the advantage of increasing transparency and reliability since it is shared with all peers in the blockchain network. In addition, the proposed model was implemented with Hyperledger Fabric and analyzed. The results of the analysis showed that digital evidence stored in the proposed model could provide high reliability.

However, this study has not yet implemented user interface and distributed application for user convenience. Nevertheless, the model proposed in this study could contribute to lowering the threats present in the transmission and management of digital evidence in Korea and increasing the reliability of digital forensic.

Acknowledgement

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2017R1D1A3B03029906), and this work was supported by the NRF grant funded by the Korea Government (MSIT) (No. 2018 R1A5A7023490). This research was supported by the Ministry of Science and ICT, Korea, under the Information Technology Research Center support program (No. IITP-2020-2020-0-01789) supervised by the Institute for Information & Communications Technology Planning & Evaluation (IITP).

References

[1] S. Psyne, “DNA link traps girl’s killer after 21 years,” 2002 [Online]. Available: https://www.telegraph.co.uk/news/uknews/1393847/DNA-link-traps-girls-killer-after-21-years.html.

[2] CNN Editorial Research, “O. J. Simpson fast facts,” 2020 [Online]. https://edition.cnn.com/2013/04/12/us/o-j-simpson-fast-facts/index.html.

[3] S. H. Moon, “'Preservation of evidence and forensic investigation', The solution that solved the mystery of Hwaseong serial killing,” 2019 [Online]. Available: http://www.ilyo.co.kr/?ac=article_view&entry_id= 347949.

[4] Korea National Police Agency, “Police White Paper,” 2018 [Online]. Available: https://www.police.go.kr/www/open/publice/publice06_2018.jsp.

[5] H. Ji, "Arrest of criminal using CCTV," 2015 [Online]. Available: https://www.mk.co.kr/news/society/view/2015/04/392686.

[6] S. K. Lee, "Implication of evidence law in the chain of custody of real evidence," *Journal of Police Science*, vol. 11, no. 3, pp. 55-84, 2011.

[7] H. S. Tak and W. S. Lee, "A study on a model frame for the integration of digital forensic processes," Korean Institute of Criminology, Seoul, Korea, 2016.

[8] H. H. Jung, "Management from the perspective of the life cycle of digital evidence," *Journal of Digital Forensics*, vol. 10, no.1, pp. 1-20, 2016.

[9] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the 13th EuroSys Conference*, Porto, Portugal, 2018.

[10] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008 [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[11] J. K. Lee, "A docker container case study for implementing block chain distributed general ledger," *Korean Computers and Accounting Review*, vol. 16, no. 1, pp. 27-41, 2018.

[12] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings of 2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, 2017, pp. 557-564.

[13] K. Ahn and H. Seo, "User verification system for improving blockchain node reliability," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 22, no. 9, pp. 1264-1270, 2018.

[14] K. Rilee, "Understanding Hyperledger Fabric endorsing transactions," 2018 [Online]. Available: https://medium.com/kokster/hyperledger-fabric-endorsing-transactions-3c1b7251a709.

[15] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352-375, 2018.

[16] J. K. Lee, "An exploratory case study distributed ledger processing using IBM Bluemix Blockchain," *Korean Computers and Accounting Review*, vol. 15, no. 1, pp. 25-38, 2017.

[17] Hyperledger Fabric: A Blockchain Platform for the Enterprise [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.2/.

[18] Docker Inc., "What is container?," 2020 [Online]. Available: https://www.docker.com/resources/what-container.

[19] M. Kim, S. Oh, and C. S. Hong, "Digital trading system using Hyperledger Fabric block chain open source," in *Proceedings of 2018 Korea Computer Congress*, 2018 pp. 1913-1915.

[20] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing Hyperledger Fabric blockchain platform," in *Proceedings of 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Milwaukee, WI, 2018, pp. 264-276.

Junho Jeong **https://orcid.org/0000-0003-4963-0057**

He received the B.S. degree from the Department of Computer Science and Engineering, Dongguk University, Seoul, Korea, in 2007, and M.S. and Ph.D. degrees from the Department of Computer Science and Engineering, Dongguk University, Seoul, Korea in 2009 and 2015, respectively. He was a research professor of Electronic Commerce Institute, Dongguk University, Gyeongju, Korea, from 2015–2019. And he was a research professor of Department of Computer Science and Engineering, Dongguk University, Seoul, Korea until 2019 Aug. Currently, he is an assistant professor of the Department of Computer Science and Engineering, Kongju National University, Cheonan, Korea. His research areas include computer security, privacy preserving, distributed system, network security, and secure software.

Donghyo Kim **https://orcid.org/0000-0001-8889-275X**

He received Bachelor's degree in School of Computer Science and Engineering from Dongguk Computer Science Institute in 2017. Also, currently he is a master student in Department of Computer Science and Engineering, Dongguk University, Seoul, Korea. His current research interests include blockchain, smart contract security and software security.

Byungdo Lee **https://orcid.org/0000-0002-2430-5891**

He received the B.A. degree from the Department of Police Administration, Dongguk University, Seoul, Korea, in 2012, and M.A. and Ph.D. degrees from the Department of Police Administration, Dongguk University, Seoul, Korea in 2014, and 2017, respectively. He was a research professor of Development of Smart Community Policing System (Googi) Research Center, Dongguk University, Seoul, Korea. Currently, he is an assistant professor of the Department of Police Science, Seoul Digital University, Seoul, Korea. His research areas include police science, criminal justice, juvenile delinquency and criminology.

Yunsik Son **https://orcid.org/0000-0002-2580-4393**

He received the B.S. degree from the Department of Computer Science and Engineering, Dongguk University, Seoul, Korea, in 2004, and M.S. and Ph.D. degrees from the Department of Computer Science and Engineering, Dongguk University, Seoul, Korea in 2006 and 2009, respectively. He was a research professor of Department of Brain and Cognitive Engineering, Korea University, Seoul, Korea, from 2015–2016. Currently, he is an assistant professor of the Department of Computer Science and Engineering, Dongguk University, Seoul, Korea. Also, His research areas include secure software, programming languages, compiler construction, and mobile/embedded systems.